

STATUS OF CLAIMS

Claims 1 - 10 are pending.

Claims 1 – 10 stand rejected.

Claims 3 and 4 have been cancelled without prejudice herein.

New Claim 29 has been added herein.

REMARKS

Claims 1 – 10 stand rejected under 35 U.S.C. 112, first paragraph. Claims 1-10 stand rejected under 35 U.S.C. 103(a). Applicant respectfully requests reconsideration and removal of these rejections for at least the following reasons.

35 U.S.C. 112, First Paragraph Rejections

Claims 1-10 stand rejected under 35 U.S.C. 112, first paragraph, as allegedly failing to comply with the enablement requirement. In support thereof, the Office action argues, “the exact function to generate each individual encryption key based upon said three parameters disclosed (i.e., public key, private key and synchronizing indicator) is not specifically defined in the specification.” Applicant traverses this rejection.

First, whether or not the present specification defines “an exact function to generate each individual encryption key from said three parameters disclosed” is not determinative of whether or not Claims 1-10 satisfy the enablement requirement of 35 U.S.C 112, first paragraph. Rather, the pertinent inquiry is whether one reasonably skilled in the art could make or use the invention from the disclosures in the application coupled with information known in the art without undue experimentation.

In re Wands, 858 F.2d at 737, 8 USPQ2d at 1404 (Fed. Cir. 1988); See also *United States v. Telectronics, Inc.*, 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988). Applicant submits the application does enable one reasonably skilled in the art to make or use the invention from the disclosures in the application coupled with information known in the art without undue experimentation.

Such an approach is explicitly provided in the present specification, where for example, Party A uses a received second public key (P_{KB1}) and synchronizing indicator (MI_{B1}) in combination with the first private key (P_{RA1}) to determine, and retain, an initial encryption key (E_{A1}). For non-limiting purposes of further explanation only, it is well known that publicly available data and privately held data may be used to generate keys useful for encryption. For example, the present application explicitly acknowledges, “[m]embers of [a] secure communication network can ... use a received public key and their own retained private key to generate an encryption key that can be used to encrypt sensitive informational data items.” *Page 2, lines 13-15.* In the same paragraph, the present application explicitly refers to United States Patent No. 4,200,770 as an example.

The above-identified patent teaches that a secure key generator 21 can generate a secure key K using a signal Y_2 that was received over an insecure communications channel 19 (e.g., publicly received) in addition to privately held signals q, a, X_1 . See, e.g., col. 4, *lines 1-50.* This patent also teaches a secure key generator 22 can generate the same secure key K using signals Y_1 , q and a that were received from an insecure communications channel 19 (e.g., publicly received) in addition to privately held signal X_2 . See, e.g., col. 4, *lines 1-50.*

Further, it is well known that key K may merely take the form of a sequence of random letters or digits. See, e.g., U.S. Patent 4,200,770, col. 3, 57-59. Thus, the present application clearly explains that synchronizing indicators are used to “provide a random element to the encrypt process to prevent a same plain-text message that is encrypted at two different times from producing the same encrypted message.” See, e.g., page 7, lines 4-7. For example, the present application clearly indicates that the synchronizing indicator can simply alter the starting position of the encoding sequence within the bits of a public key. See, e.g., page 7, lines 8-11. Further yet, the present application explains that a synchronizing indicator can be used to produce different encoded messages from a same plain-text message. See, e.g., page 7, lines 11-12.

In view of the foregoing, Applicant submits the present application clearly enables one possessing an ordinary skill in the pertinent arts to make and use the claimed invention, including generating an encryption key based upon a public key, private key and synchronizing indicator by altering the starting position of the encoding sequence within the bits of a public key. Reconsideration and removal of this 35 U.S.C. 112 first paragraph rejection is requested.

35 U.S.C. 103(a) Rejections

Claims 1-10 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro (United States Patent No. 6,009,176) in view of Bjerrum (United States Patent No. RE.36,310). Applicant respectfully requests reconsideration and removal of these rejections for at least the following reasons.

35 U.S.C. §103(a) sets forth in part:

[a] patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

To establish a *prima facie* case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. See, *MPEP 2143.03*; see also, *In re. Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

Referring first to Claim 1, it recites in part, “[a] method for facilitating secure communications among at least two parties over a communication network, comprising: retaining a first private key and transmitting a corresponding first initial public key and synchronizing indicator.” Applicant submits Gennaro and Bjerrum fail, in any combination, to teach or suggest such a process.

The Office action argues Gennaro teaches retaining a first private key and transmitting a corresponding first public key and synchronizing indicator in column 10, lines 4-7. The Office action argues the digital signature of the hash value corresponds to the synchronizing indicator. Applicant traverses these assertions.

As an initial matter, Applicant previously amended Claim 1 to recite transmitting a corresponding “synchronizing indicator” (and not just any data). The Examiner must rely on the applicant’s disclosure to properly determine the meaning of this limitation. *Markman v. Westview Instruments*, 52 F.3d 967, 980, 34 USPQ2d 1321, 1330 (Fed. Cir.) (*en banc*), aff ’d, U.S., 116 S. Ct. 1384 (1996). Limitations appearing in the specification but not recited in the claims are not read into the claims, but the claims

must be interpreted “in view of the specification”. See, e.g., *E-Pass Techs., Inc. v. 3Com Corp.*, 343 F.3d 1364, 1369, 67 USPQ2d 1947, 1950 (Fed. Cir. 2003). Accordingly, the recited “synchronizing indicator” must be interpreted in light of the specification to determine its meaning. In fact, correlating each claim limitation to all portions of the disclosure that describe the claim limitation is a necessary step to ensure correct claim interpretation. See, e.g., *MPEP 2106(c)*.

As set forth above, the present application clearly and unambiguously explains that synchronizing indicators are used to “provide a random element to the encrypt process to prevent a same plain-text message that is encrypted at two different times from producing the same encrypted message.” See, e.g., *page 7, lines 4-7*. For example, the present application clearly and unambiguously explains a synchronizing indicator can simply alter the starting position of the encoding sequence within the bits of a public key. See, e.g., *page 7, lines 8-11*.

In contrast, a digital signature of a hash value is not a synchronizing indicator. A digital signature of a hash does not prevent a same plain-text message that is encrypted at two different times from producing the same encrypted message. Instead, a digital signature of a hash, as explained by Genarro itself, is commonly used simply to authenticate the message. See, e.g., *col. 10, lines 3-12*. In fact, to the opposite, in order to allow a message to be authenticated, it is crucial that it

lead to a predictable result. Thus, Genarro fails to teach, or suggest, the recited use of synchronizing indicators at all.¹

Bjerrum fails to remedy at least this shortcoming of Genarro. The Office action argues Bjerrum teaches using a received public key and synchronizing indicator in combination with a first retained private key to determine and retain a first encryption key in column 18, lines 47-62 and column 37, lines 52-56. Applicant traverses this assertion as well. Instead, these portions of Bjerrum merely teach that asymmetric cryptography uses public transformation and secret transformation keys (See, e.g., col. 18, lines 47-51) and, that an asymmetrical cryptography system can be used for concealment, authentication and generating digital signatures. See, e.g., col. 18, lines 52-62 (*i.e., uses his secret key SA to receive secret messages, and his digital signature and other person's public key to send secret messages*). Finally, column 37, lines 52-57 of Bjerrum merely teach that encryption key(s) stored in first and second electronic cards include(s) a random encryption key made by use of a previously exchanged random number (e.g., a public key).

Accordingly, like Genarro, Bjerrum merely teaches conventional use of public/private key cryptography and digital signatures, and fails to teach, or suggest, Applicant's claimed use of "synchronizing indicators". In view of the foregoing, Applicant submits Bjerrum fails to remedy the shortcomings of Genarro,

¹ New Claim 29 makes this distinction even more clear. For purposes of completeness, no new matter has been added. New Claim 29 finds support in the passages described above, by way of non-limiting example only.

such that the combined teachings of Genarro and Bjerrum fail to render present Claim 1 unpatentable.

Further, even *assuming arguendo* that one could properly equate the digital signatures of Genarro and Bjerrum to the recited “synchronizing indicators” of Claim 1, (which one in fact cannot), the combined teachings of Genarro and Bjerrum still fail to satisfy the limitations of Claim 1. For example, Claim 1 further recites, “using a received second public key and second synchronizing indicator in combination with said retained first private key to determine, and retain, a first encryption key.” Genarro fails to teach, or suggest, using a digital signature to determine an encryption key. Instead, the relied upon portion of Genarro explicitly teaches merely authenticating the message using the digital signature. See, col. 10, lines 3-12. Bjerrum, in contrast to the claimed invention, recites using a user’s own private key to receive messages, and not the digital signature. See, e.g., col. 18, lines 54-62; see also, col. 37, lines 52-57 (*which explicitly recites storing an encryption key made by use of a previously exchanged random number, and not a digital signature*). For purposes of completeness, if a user can receive secure messages using only his secure key (SA), clearly the digital signature is not used to determine the encryption/decryption key – as the key need be ascertained to access the secure message in the first place.

Further yet, Claim 1 additionally recites, in part, “encrypting at least said third synchronizing indicator using said first encryption key.” Contrary to the assertions on page 5 of the Office action, neither Genarro nor Bjerrum teach, or suggest, further encrypting any digital signature of a hash value. Rather, steps m and n of Claim 31 of

Bjerrum (col. 37, lines 9-13) merely recite encrypting combined random numbers to generate an authenticity message, which is transmitted. This merely equates, at most, to Genarro's digital signing of a hash itself, and does not teach, or suggest, further encrypting a digital signature – which is asserted in the present Office action to equate to the encrypted "synchronization indicator" recited in the present claims.

Accordingly, Applicant submits the cited art of record fails in any combination, to teach, or suggest, each of the limitations of Claim 1, and hence fails, as a matter of law, to anticipate Claim 1. Wherefore, Applicant respectfully requests reconsideration and removal of the rejections of Claim 1 for at least the foregoing reasons. Applicant also requests reconsideration and removal of the rejections of Claims 2-10 as well, at least any virtue of these claims' ultimate dependency upon a patentably distinct base Claim 1.

CONCLUSION

Applicant believes he has addressed all outstanding grounds raised in the outstanding Office action, and respectfully submits the present case is in condition for allowance, early notification of which is earnestly solicited.

Should there be any questions or outstanding matters, the Examiner is cordially invited and requested to contact Applicant's undersigned attorney at his number listed below.

Respectfully submitted,


Edward J. Howard
Registration No. 42,670

Plevy, Howard & Darcy, P.C.
PO Box 226
Fort Washington, PA 19034
Tel: (215) 542-5824
Fax: (215) 542-5825